

stripe cards. However, in some circumstances a thief or counterfeiter may be able to access the information stored in proximity or smart cards.

**[0013]** The present invention is designed to preclude skimming (i.e., stealing) of cardholder information when proximity, contactless or smart cards are in transit, for example, sent to the cardholders through public mail.

**[0014]** The on-card chips have electronic circuits, which exploit electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to communicate with card reader units (e.g., Point of Sale devices). A card reader unit may include an RF antenna and a transceiver. The reader unit emits radio waves, and when a proximity, contactless or smart card is placed within the range of the card reader unit, the on-card chip responds and starts sending data to the reader unit. The on-card chips themselves may come in a wide variety of size, shapes and forms but have common attributes; each includes low-energy broadcast circuitry, programmable data storage and operating circuitry. The on-card chips may be with and without batteries, and they can be read only or read/write. Typically, on-card chips without batteries (passive circuits) are smaller and lighter than those that are with batteries (active circuits), and less expensive. The passive on-card chip circuits are powered and activated by the reader units. In either case, when activated on-card chip circuits can broadcast stored information over radio frequency waves.

**[0015]** At least theoretically, it is possible for an unauthorized person or fraudster to use a card reader or similar RF device to extract cardholder information stored in an on-card chip in a manner similar to using an unauthorized magnetic stripe card reader to skim information from magnetic stripe cards. In the case of proximity, contactless or smart cards, a potential opportunity for accessing card information arises when card issuers sent cards by the to cardholders by mail, for example, in conventional postal envelopes or mailing packages. The unauthorized person or fraudster may use a card reader or similar RF device to activate the on-chip card and extract card information while the card is in transit. The unauthorized person may literally do so without opening the envelope—possibly even while the card is still in a mailbox.

**[0016]** According to the present invention, the cards are sent to cardholders enclosed in mailers with RF-shielding, which prevents external radio frequency waves from penetrating the mailer and activating or communicating with the enclosed cards. An exemplary mailer **100** may include a conventional paper envelope **110** and/or paper or cardboard insert **120** to which the proximity, contactless or smart card **140** is tacked onto or attached. (See FIG. 1). RF-shielding material **130** is disposed on paper envelope **110**, for example, on interior surfaces proximate to the enclosed card. Alternatively or additionally, RF-shielding material **130** may be disposed on insert **120**. RF shielding material **130** may be any suitable material that interferes with the transmission of RF frequency waves. The suitable RF shielding materials may, for example, include conductive inks, metallic films or paper, wire screens, and wire mesh pouches. In some cases, RF-shielding material **130** may simply be a metallic adhesive

(e.g., a conductive rubber cement) that can be used to tack the enclosed smart card in position. It will be understood that according to the present invention, RF-shielding material **130** is selected and its geometrical disposition is designed based on known electromagnetic effects (e.g., skin depth) so that it (RF-shielding material **130**) effectively interferes with RF signals to or from the on-card chip **150**. Thus, the inventive mailer prevents unauthorized detection or reading of the enclosed card.

**[0017]** It will be understood that the foregoing is only illustrative of the principles of the invention, and that various modifications can be made by those skilled in the art without departing from the scope and spirit of the invention.

1. A method for transporting a payment card having an on-card microchip, the method comprising:

providing a mailer having RF-shielding material disposed therein; and

enclosing the payment card having an on-card microchip in the mailer, wherein the RF-shielding material is disposed in a manner so that it interferes with external RF signals from reaching the on-card microchip in the mailer.

2. The method of claim 1 wherein the mailer comprises an envelope, and wherein the RF-shielding material is disposed on an interior surface portion of the envelope.

3. The method of claim 1 wherein the RF-shielding material is disposed on the envelope proximate to the enclosed the payment card.

4. The method of claim 1 wherein the mailer comprises an envelope, and wherein the RF-shielding material is disposed on an insert to which the payment card is attached.

5. The method of claim 1 wherein the RF-shielding material comprises a conductive ink.

6. The method of claim 1 wherein the RF-shielding material comprises a metallic film.

7. The method of claim 1 wherein the RF-shielding material comprises a wire mesh.

8. A system for preventing unauthorized skimming of information from a payment card in transit, the payment card having an on-card microchip that is activated by and communicates via radio frequency signals, the system comprising:

a mailer enclosing the payment card in transit; and

RF-shielding material disposed in the mailer proximate to the enclosed card, wherein the RF shielding material is disposed in a manner so that it interferes with external RF signals from reaching the on-card microchip enclosed in the mailer.

9. The system of claim 8 wherein the mailer comprises an envelope, and wherein the RF-shielding material is disposed on an interior surface portion of the envelope.

10. The system of claim 8 wherein the mailer comprises an envelope, and wherein the RF-shielding material is disposed on an insert to which the payment card is attached.

11. The system of claim 8 wherein the RF-shielding material comprises a conductive ink.

12. The system of claim 8 wherein the RF-shielding material comprises a metallic film.

\* \* \* \* \*